

Architecture and Standards

January 9, 2001

Discussion of the Issues:

Teams working in the security, network, and Web areas have submitted the following standards and policies:

1. *Intrusion Detection System Standard:* Approved by SISC on September 13, 2000. There is no fiscal impact to the State of Utah. This standard was previously submitted to the ITPSC for comment. This standard is submitted for ITPSC approval.
2. *VPN Standard:* Pending before SISC and submitted for comment on September 13, 2000. Fiscal impact is minimal and was addressed in the fiscal impact statement for the Firewall Standard. This standard was previously submitted to the ITPSC for comment. This standard is submitted to the ITPSC for approval.
3. *Web Standards Revision:* A working group of the ITPSC was convened to revise the State Web Standards approved by the ITPSC two years ago. This standard was previously submitted to the ITPSC for comment. Comments have been incorporated in this draft and a fiscal impact note has been included. This standard is submitted for approval.
4. *State Information Security Charter.* SISC has developed this document for signature by the Governor as a statement of security direction for all agencies of State government. This Charter has been reviewed by agency IT managers and SISC members and comments have been incorporated in the document. SISC approved this Charter on January 8, 2001. Fiscal impact to the State is minimal. This charter is submitted for endorsement and/or approval.
5. *State Information Security Policy.* Development of this policy began in March 2000. The document has been submitted for review and comment to IT Managers/Directors, SISC, and other relevant state security committees, and the State Auditor's office. Several large agencies have provided comprehensive review and comment on the policy. SISC approved the policy on January 8, 2001. Fiscal impact to the State is minimal. This policy is submitted for approval.
6. *State Security Policy Development Methodology.* This document is provided as an overview of the process being utilized to develop an overall set of security policies for the State of Utah. It is provided as an information item for ITPSC members.
7. *State Firewall Policy.* This document has been developed by SISC as a part of the Security Integration Project initiated by SISC in January 2000. The document sets policy for firewall implementations in government agencies and is based upon practical experience and best practices from the firewall portion of the Security Integration Project. Fiscal impact to the State is minimal. This policy is submitted for comment.
8. *State Network Access Policy.* SISC and the Network Access Work Group are responsible for this document. This policy was developed in response to the ITPSC assignment to the Technical Architect to look at requirements and policies for providing access to the State network. It is the first of several documents that will formulate the basis for a comprehensive approach to network access by agencies, extranet partners, and other relevant third parties. Fiscal impact to the State has not been analyzed. This policy is provided for comment.

Recommended Actions:

Approval of items 1-5, information only on item 6, and discussion on items 7 through 8.